CSX PRACTITIONER CERTIFICATION FACT SHEET

CSX Practitioner Certification (CSXP) was named 2016 Top Professional Certification program in the SC Awards, and was named a finalist in 2018. It remains the first and only *comprehensive* performance certification to assess one's ability to perform globally validated cybersecurity skills spanning five security functions – Identify, Protect, Detect, Respond and Recover.

The CSXP exam has been updated for 2018 to reflect the job tasks of today's cybersecurity practitioner. CSXP has transitioned to remote proctor delivery to meet global demand and afford greater scheduling flexibility without traveling to a physical test center.

Performance Certification

Employers, governments and academia widely recognize the shortcomings of traditional multiple-choice exams. Whereas not all certifications are conducive to performance assessment, the cybersecurity industry demands it. No two corporate networks are identical, meaning today's cybersecurity practitioner must adapt to ever-changing environments. CSXP exam takers cannot simply "cram" – they must perform tasks using widely available security tools and, in doing so, have demonstrated aptitude for performing security tasks in dissimilar environments.

About the Exam

The four-hour CSXP exam consists of 30 tasks. It requires candidates to demonstrate critical cybersecurity skills in a live, virtual environment assessing candidates' analytical ability to identify and resolve network and host cybersecurity issues by applying foundational cybersecurity knowledge and skills required of an evolving cyber first-responder. Content areas covered include:

Business and Security Environment (ID)	**23%**
Business Environment	
Digital Infrastructure	
Enterprise Architecture	
Data and Digital Communication	
Security Environment	
Network	
Operating Systems	
Applications	
Virtualization and Cloud	
Operational Security Readiness (PR)	**23%**
Protection	
Digital and Data Assets	
Ports and Protocols	
Protection Technologies	
Identity and Access Management	
Configuration Management	
Preparedness	
Threat Modeling	
Contingency Planning	
Security Procedures	

Threat Detection and Evaluation (DE)	27%
Monitoring	
Vulnerability Management	
Security Logs and Alerts	
Monitoring Tools and Appliances	
Use Cases	
Penetration Testing	
Analysis	
Network Traffic Analysis	
Packet Capture and Analysis	
Data Analysis	
Research and Correlation	
Incident Response and Recovery (RS&RC)	**27%**
Incident Handling	
Notifications and Escalation	
Digital Forensics	
Mitigation	
Containment	
Attack Countermeasures	
Corrective Actions	
Restoration	
Security Functions Validation	
Incident Analysis and Reporting	
Lessons Learned and Process Improvement	

Preparation

Candidates are strongly encouraged to review the CSXP exam blueprint and other publicly available information located at https://cybersecurity.isaca.org/csx-certifications/csx-practitioner-certification. ISACA does offer training opportunities to aid preparation but they should not be considered all-encompassing.

Contact: *communications@isaca.org*
Laurel Nelson-Rowe, +1.847.660.5566
Kristen Kessinger, +1.847.660.5512
Michelle Micor, +1.847.385.7217
Jay Schwab, +1.847.660.5693